

INTELLIGENCE

# U.S. vs Iran, a Cybersecurity Update



Published 3 years ago on January 11, 2020  
By **Dr.Luciano Maqaldi**

PUBLICATIONS

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish.

Accept

Reject

[Read More](#)



Comments

The relationship between the United States and Iran has perhaps reached a very low level in recent weeks, following the **1979 Khomenist Revolution** and the **occupation of the US Embassy in Tehran** by Iranian students.

According to American sources, on 20th June the United States launched offensive cyber-operations against Iranian intelligence computer systems, the same day that the US President, Donald J. Trump, had before ordered a military attack and then revoked the order before it actually left.

**The United States Cyber Command** – a department recently promoted by Trump as a unified combat command under the direction of the Department of Defense – allegedly attacked the computer systems used to control missile and rocket launches.

Such a cyberattack would have been the **White House's** response to the actions of the Iranian authorities who, the day before, had shot down an American spy drone – a **Global Hawk** produced by **Northrop Grumman** – as it was guilty of violating the airspace of the Islamic Republic.

After accusations and threats to each other, the US President decided to impose new sanctions on Iran and **Ayatollah Ali Khamenei**. That was not welcomed by the Government of Tehran, which spoke, earlier, of “end of diplomatic path with the United States” and announced that it had exceeded the uranium enrichment limit imposed by the **JCPOA – Joint Comprehensive Plan of Iran Nuclear Deal** – from which the United States unilaterally exited in May 2018.

It remains to be seen, therefore, after the escalation of the last few weeks, whether the United States will try to make more and more use of cyber-attacks to solve the delicate international issues, primarily the Iranian one.

After the cyber-space was recognized as a strategic domain by NATO in 2016, on par with land, water, sky and space, it has been increasingly seen that countries use this domain to plead their own interests and also to carry out operations – this new type of military activity should not come as a surprise, because you only have to look at the **National Cyber Strategy**, published in September 2019 by the US, which shows that there has been a paradigm shift from what was the protection of American interests in the cyber space, moving from a more classical deterrence to the purpose of defence to a more offensive deterrence.

Armenia's Existential Threats and Strategic Issues



Rethinking Iran: 1979-2019



A character assassination campaign against the Crown Prince



## LATEST



ENVIRONMENT / 2 hours ago

**For Somalia, nature is key to lasting peace**



RUSSIA / 4 hours ago

**Mikhail Bogdanov's Passion for Africa and the Critical Russia's Policy Debates -Part 1**



FINANCE / 7 hours ago

**\$500M World Bank Financing to Help Bangladesh Improve Disaster Preparedness**



REPORTS / 9 hours ago

**Reforms Can Support Inclusive Growth in Turbulent Economic Times**

The fact that this document was only published last September suggests that the field of cybersecurity is fundamentally new and still to be explored.

On the one hand, cybernetic space is a totally man-made space and where you can have very high levels of ambiguity, through non-identification strategies from where attacks start, on the other hand, it is one of the most unregulated space at the level of behaviour that all countries should adopt with the specific responsibilities in cyber-operations.

This is a field in which the international law must be adapted as it is vital to understand how international law applies to the cyber-space and to see how it can be applied in practice: there is a long-time discussion between experts in the United Nations about cyber-space and, moreover, you can conduct operations that may fall into the category of attacks that are below the threshold of the use of force. So, it is still unclear whether a cyber-attack can be responded to with a classic attack by using any classic military tools.

That is why American cybersecurity policy has changed in recent years, starting with the different pillars on which the **National Cyber Strategy** is based:

- 1) defending the homeland by protecting networks, systems, functions and data; promote American prosperity by fostering a secure digital economy and promoting strong domestic innovation;
- 2) preserving peace and security by strengthening the ability of the United States – along with allies and partners – to deter and, if necessary, punish those who use cyber-tools for malicious purposes;
- 3) expansion of American influence abroad to extend the key principles of an open, reliable and secure Internet.

Within the cyber-space, the United States have adopted a so-called “continuous engagement” – an ongoing commitment to counter possible threats even before they can materialize through targeted attacks, with the transition from a defensive to an offensive approach, with the American presence in the cyber-space that will more and more increase in order to actively dissuade potential enemies.



FINANCE / 14 hours ago

**Poland's Growth Potential Could Reach 4 Percent with Reforms and Investments**



WORLD NEWS / 16 hours ago

**CFP: IV Eurasian Research on Modern China and Eurasia Conference**



AMERICAS / 18 hours ago

**China's vision of the results and outputs of the Jeddah summit and the American role**

Historically, the United States are not new to carrying out cyber-attacks on Iran, in fact, as early as 2010, the United States and Israel are believed to have spread a virus, created by the US Government, to slow down the process of enriching uranium in Iran's nuclear power plants.

That cyber-attack of the United States against the Iranian intelligence unit is part of a context that has seen Washington's intensifying cyber-operations also against Russia and Iran – it is important to be aware of the cybersecurity space for their own interests and that they have had a particularly aggressive posture in this area.

The United States and Iran are two of the world's most advanced, active and capable hacking powers at a time when governments regularly use cyber-attacks to achieve important goals and shape geopolitics.

Tensions between the two countries and their allies have produced a long history of extraordinary cyber-attacks in addition to traditional kinetic warfare – for these reasons, Iran's revenge for the killing of General Qassim Suleimani could also be served on the ground of cyber-war.

**Christopher Krebs, director of the Cybersecurity and Infrastructure Security Agency – CISA – of the U.S. Department of Homeland Security**, warned the entire community to re-investigate Tehran's tactics, procedures and techniques in detail in cyberspace, after reporting the increase in the activity of malicious cyber-attacks directed against the American companies and government agencies.

The hackers of the Iranian regime have increasingly used **destructive windshield wipers** in order to spear phishing, email scam to gain unauthorized access to sensitive data – it is a hackerial attempt to decode a common user password across multiple accounts before switching to a second password that allows you to circumvent account lockouts.

This is an attack that leverages the likelihood that people can use the same username and password to access multiple applications, sites, and services – in fact, cyber-criminals are able to get the details of stolen accounts from a platform and implement the bots needed to log into many other accounts with the same credentials.

Once they have found a way to log in, the criminals will break the account by making fraudulent purchases or stealing confidential information – before the 2015 nuclear deal was negotiated between the United States, Iran, Europe, Russia and China, Iranian hackers regularly targeted American financial companies and critical infrastructure.

Over the past year, Iran and the United States have repeatedly targeted each other in hacking operations – Iranian government hackers have attempted to breach President Trump's re-election campaign: in fact the U.S. Cyber Command reportedly warned against Iran's paramilitary force attacks during a period of high tensions, earlier this year.

More than 150 American sites have already been victims of defacement by Iranian hackers also because of the **supreme leader, Ayatollah Ali Khamenei**, had promised "a strong vengeance" for Suleimani's killing – this is a modern conflict, to date not only threatened but it is a long-time a cyber war – in recent days, hackers of Tehran have hacked the website of the **Federal Depository Library Program – FDLP** – with a defacement operation, leaving a message stating that "this is only a small part of Iran's cyber-capabilities."

The attack targeted a "weak" target, but it is a sign that the Islamic Republic's cyber-army has been activated to strike US-linked targets, any critical infrastructure in particular..

The U.S. cyber-army believe, in fact, that the attacks could take place in five ways:

- DDoS attacks, in which you flood a site with access requests and crash it.
- data deletion (or wiper attack), actions to delete data in infected databases.
- attacks on industrial control systems, information-related operations and as well as cyber espionage.

The latter two to steal data for use then in physical, military actions – for example, by committing targeted murders or attacks on infrastructure.

But the Islamic Republic could suffer from the American reaction far more damage than it could cause: it has already happened in the past, as confirmed by the **head of the "cyber police" in Tehran, General Kamal Hadianfar**, who admitted that Iran in 2017 suffered 296

serious cyber-attacks against paramount infrastructures and on several occasions some experts in the field were mysteriously dead.

In conclusion, after sanctions and threats on both sides, could we really lead to an escalation of cyber-attacks and, because of that, does it seem to be a new Cold War ?

---

## Share this:



RELATED TOPICS: [#CYBERSECURITY](#) [#IRAN](#) [#USA](#)

DON'T MISS



**Beijing's Export of Surveillance Technology**

UP NEXT

**Anti-Russian Ideology of Central Asian Salafi-Jihadi Groups: Causes and Consequences**



**Dr.Luciano Magaldi**

Dr. Luciano Magaldi Orta Nova, after his PhD in Cloud Computing at Cloud University by Rackspace in San Antonio, Texas, a Master of Science in Security Engineering at Cibrary Faculty of Washington, the Tesol certificate at Arizona State University in Tempe, a Bachelor of arts in Interpreting and Translating at Lus Pio V in Rome, an SEO specialization at the University of California Davis (UC Davis), a DSA specialisation at the University of London, an ETL specialisation at the Universitat Aut'onoma of Barcelona, an academic diploma in Forensic Sciences at Oxford Royale Academy, a specialising certificate in American Politics at Harvard Kennedy School, a professional certificate in mathematics at Stanford University, a Copyright Law certificate at MIT in Cambridge, used to work for Google Ireland in Dublin, Apple European campus in Cork, Ireland, and Amazon Slovakia in Bratislava. Dr. Luciano Magaldi finally obtained his specialisation in journalism at Michigan State University School of Journalism. His career as a journalist began writing articles for AgoraVox France and AgoraVox Italia about world politics, military issues and cyber-tech.

---

**YOU MAY LIKE**



China's vision of the results and outputs of the Jeddah summit and the American role



China and the CIA Project of right Judgments of Future Predictors



The espionage war between China and the USA



Biden's Middle East Tour: A Mockery of the American Foreign Policy



Endgame: Time, History and Alternative World Futures



Behind President Putin's visit to Iran

COMMENTS

---

**INTELLIGENCE**

# China and the CIA Project of right Judgments of Future Predictors



Published 23 hours ago on July 18, 2022

By **Dr.Nadia Helmy**

The (Project of Sound Judgments of Brilliant Future Predictors), which is funded by the "Advance Intelligence Research Projects Activity" section of the US government and the US Central Intelligence Agency (CIA), is striving to recruit, sort and employ brilliant geniuses who are able to predict the future in an unprecedented and genius way, by discovering new ways in advanced intelligence proactive thinking, which allows predicting the shape of the future and the new world order, and its network of international alliances globally

Here, the Central Intelligence Agency (CIA's accurate and right Judgments of the Future Predictors Project) believes that there are real geniuses and super-intelligent proactive

geniuses globally, who are better than others, and better prepared to predict global future events

The Central Intelligence Agency (CIA's Good Judgments of the Future Predictors Project)

CONTINUE READING

INTELLIGENCE

# The espionage war between China and the USA



Published 1 day ago on July 18, 2022

By **Dr.Nadia Helmy**

The intensity of US accusations of China of China's use of vast espionage networks behind Chinese intelligence to access information on the intellectual property of American inventions has increased. With the American assertion that Chinese espionage costs the United States of America more than \$600 billion annually in stolen intellectual property. From here, you will find full cooperation and sharing of information between students, scholars, academics, and even Chinese citizens residing in the United States of America and all its various states with the "Chinese Ministry of National Security", and all official and national institutions of the Chinese state, and cooperation with Chinese security agencies, which are fully targeted regularly meeting with Chinese scholarship students abroad, especially in the United States of America.

Here, we find that one of the most prominent American fears is China's superior ability to

CONTINUE READING

INTELLIGENCE

# India's Pakistan-bashing dossier



Published 3 days ago on July 16, 2022

By **Amjed Jaaved**

Since Pakistan announced that the Financial Action Task force was about to lift Pakistan from the “Grey List”, India was ill at ease. The dossier has tell-tale signs that it was a lame duck effort to compel the FATF to keep Pakistan at the Grey. Another stimulus for the production of the dossier was to do tit for tat to Pakistan’s dossier about India’s nefarious acts.

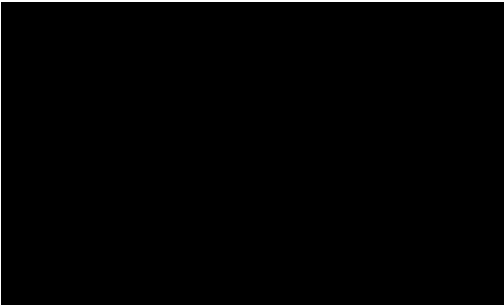
The dossier begins with rigmarole about the Jammu and Kashmir State which is a lingering dispute between India and Pakistan. India did not elaborate how it could unilaterally declare a disputed territory to be a part of the Indian Union.

### **The myth of accession**

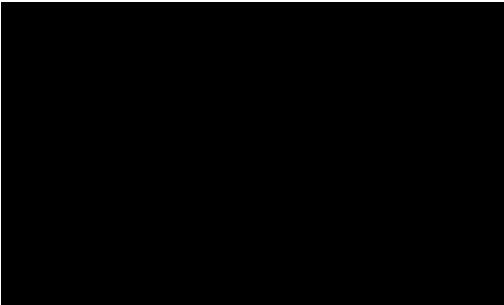
India is a signatory to the United Nations’ resolutions on the disputed Kashmir state. By annexing it violated jus *cogen* of International Law, *pacta sunt servanda*. Treaties are binding on parties. Any country that flouts an international treaty qualifies as a rogue state and

CONTINUE READING

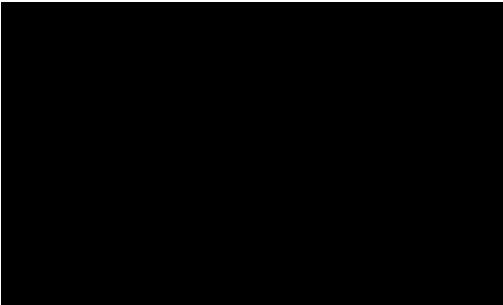
TRENDING



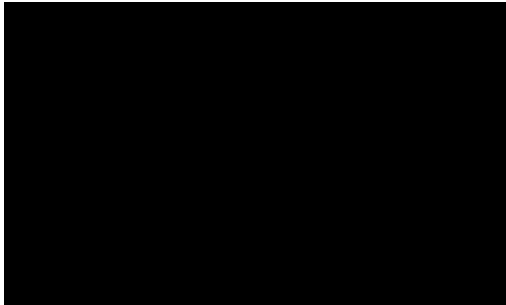
INTERNATIONAL LAW / 3 days ago  
Regulate outer space before it is too late



RUSSIA / 3 days ago  
Behind President Putin’s visit to Iran



ENERGY / 4 days ago  
The U.S. Government’s Fake Opposition to Global Warming



AFRICA / 4 days ago  
United Kingdom Pursuing Investment Projects in Africa



TERRORISM / 3 days ago  
Analyzing link between Middle Eastern politics and the rise of ISIS



REPORTS / 4 days ago  
World population to reach 8 billion this year, as growth rate slows



INTELLIGENCE / 3 days ago  
India’s Pakistan-bashing dossier



INTERNATIONAL LAW / 3 days ago  
Endgame: Time, History and Alternative World Futures



[AGENDA](#)

[BUSINESS](#)

[REGIONS](#)

[SECURITY](#)

[OUR BOARD](#)

[CONTRIBUTORS](#)

[CONTACT US](#)